Civil Action No. 6:20-cv-766

Exhibit 1

U.S. Patent 7,010,698
"Systems and Methods for Creating a Code Inspection System"
Pre-Discovery Evidence of Use for Infringement

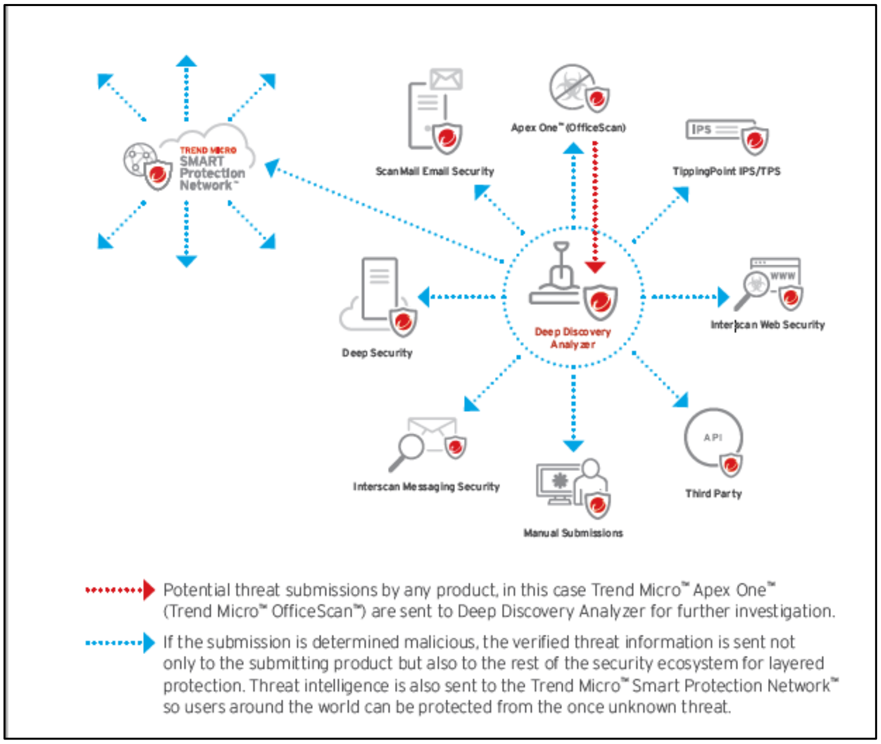
Priority Date: February 14, 2001
Note: Statements made herein are illustrative and not exhaustive

Claim Language	Where in the Accused Product(s) Each Limitation of the Asserted Claim(s) are Found
Claim 1: A code inspection system comprising:	Defendant Trend Micro's accused systems embody a code inspection system as claimed in claim 1 of the '698 patent. Trend Micro controls its accused systems for its benefit (*e.g.*, fiscal gains). Trend Micro's systems also benefit end-users of the system (*e.g.*, security and protection). For example, Trend Micro's Deep Discovery Inspector uses detection engines and custom sandbox analysis to identify potential threats and attackers (*e.g.*, code inspection). If a threat is discovered, security solutions may be updated automatically. "Trend Micro™ Deep Discovery™ Inspector is a physical or virtual network appliance that monitors 360 degrees of your network to create complete visibility into all aspects of targeted attacks, advanced threats, and ransomware. **By using specialized detection engines and custom sandbox analysis, Deep Discovery Inspector identifies advanced and unknown malware, ransomware, zero-day exploits, command and control (C&C) communications, and evasive attacker activities that are invisible to standard security defenses.** Detection is enhanced by monitoring all physical, virtual, north-south, and east-west traffic." Source: https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/inspector.html (emphasis added) "Deep Discovery Analyzer extends the value of existing security investments from Trend Micro and third parties (through a web services API) by providing **custom sandboxing and advanced analysis.** It can also provide expanded sandboxing capabilities to other Trend Micro products. **Suspicious objects can be sent to the Analyzer sandbox for advanced analysis using multiple detection methods. If a threat is discovered, security solutions can be updated automatically.**" Source: "Deep Discovery Analyzer" Datasheet, https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html (emphasis added) "Deep Discovery Analyzer is a turnkey appliance that uses **virtual images of endpoint configurations to analyze and detect targeted attacks**." Source: https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html (emphasis added)

U.S. Patent 7,010,698
“Systems and Methods for Creating a Code Inspection System”
Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001
Note: Statements made herein are illustrative and not exhaustive

As shown in the diagram below, “potential threat submissions” are sent to the Deep Discovery Analyzer. If such a submission is determined to be malicious, the entire Trend Micro Security Ecosystem and Smart Protection Network is updated for all users.



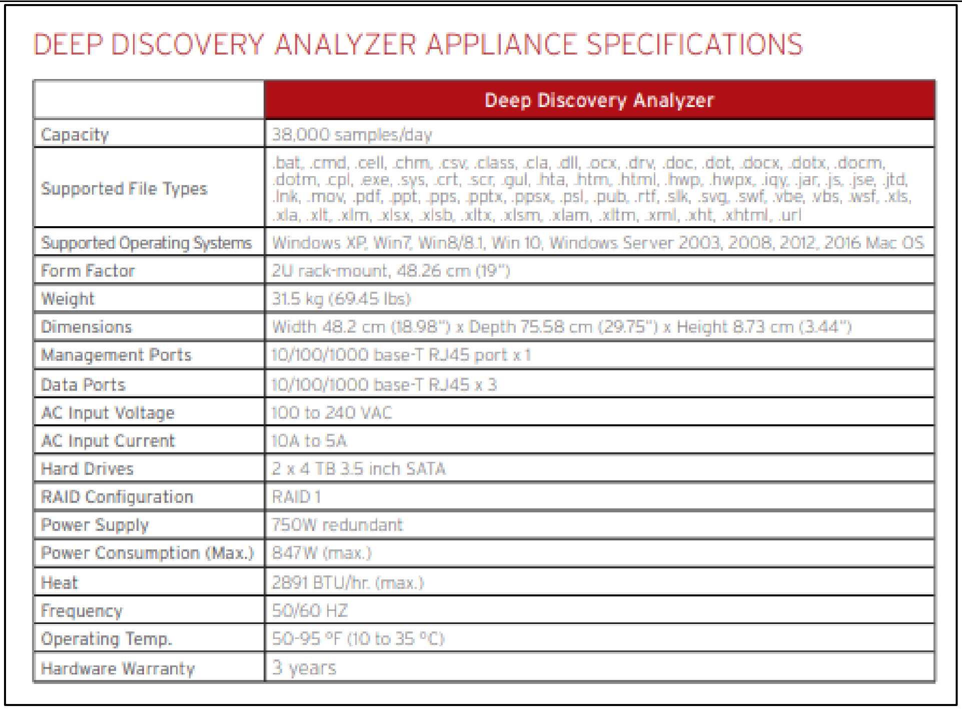
Potential threat submissions by any product, in this case Trend Micro™ Apex One™ (Trend Micro™ OfficeScan™) are sent to Deep Discovery Analyzer for further investigation.

If the submission is determined malicious, the verified threat information is sent not only to the submitting product but also to the rest of the security ecosystem for layered protection. Threat intelligence is also sent to the Trend Micro™ Smart Protection Network™ so users around the world can be protected from the once unknown threat.

Source: “Layered Security for Detection and Response” brief, www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3b-prd-img-solution-brief-1d3c9f

U.S. Patent 7,010,698
“Systems and Methods for Creating a Code Inspection System”
Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001
Note: Statements made herein are illustrative and not exhaustive



DEEP DISCOVERY ANALYZER APPLIANCE SPECIFICATIONS

	Deep Discovery Analyzer
Capacity	38,000 samples/day
Supported File Types	.bat, .cmd, .cell, .chm, .csv, .class, .cla, .dll, .ocx, .drv, .doc, .dot, .docx, .dotx, .docm, .dotm, .cpl, .exe, .sys, .crt, .scr, .gul, .hta, .htm, .html, .hwp, .hwpx, .iqy, .jar, .js, .jse, .jtd, .lnk, .mov, .pdf, .ppt, .pps, .pptx, .ppsx, .psl, .pub, .rtf, .slk, .svg, .swf, .vbe, .vbs, .wsf, .xls, .xla, .xlt, .xlm, .xlsx, .xlsb, .xltx, .xlsm, .xlam, .xltm, .xml, .xht, .xhtml, .url
Supported Operating Systems	Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, 2016 Mac OS
Form Factor	2U rack-mount, 48.26 cm (19")
Weight	31.5 kg (69.45 lbs)
Dimensions	Width 48.2 cm (18.98") x Depth 75.58 cm (29.75") x Height 8.73 cm (3.44")
Management Ports	10/100/1000 base-T RJ45 port x 1
Data Ports	10/100/1000 base-T RJ45 x 3
AC Input Voltage	100 to 240 VAC
AC Input Current	10A to 5A
Hard Drives	2 x 4 TB 3.5 inch SATA
RAID Configuration	RAID 1
Power Supply	750W redundant
Power Consumption (Max.)	847W (max.)
Heat	2891 BTU/hr. (max.)
Frequency	50/60 HZ
Operating Temp.	50-95 °F (10 to 35 °C)
Hardware Warranty	3 years

Source: “Deep Discovery Analyzer” Datasheet,
https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html

On information and belief, reasonable discovery will confirm that Trend Micro provides a code inspection system as set forth in claim 1 of the ‘698 patent, for multiple operating systems as in the datasheet above.

a code inspection management module that monitors and communicates with a protected system;

Trend Micro’s accused systems embody a code inspection management module that monitors and communicates with a protected system. For example, Trend Micro’s Deep Discovery Analyzer embodies such a module by communication with endpoints and third-party systems to determine where and if malicious content exists. Trend Micro’s Deep Discovery Analyzer is “managed with a centralized management platform, Trend Micro Control Manager,” (*e.g.*, a code inspection management module). Deep Discovery Analyzer creates custom sandboxes that match targeted desktop software configurations (etc.) (*e.g.*, a protected system).

U.S. Patent 7,010,698
“Systems and Methods for Creating a Code Inspection System”
Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001
Note: Statements made herein are illustrative and not exhaustive

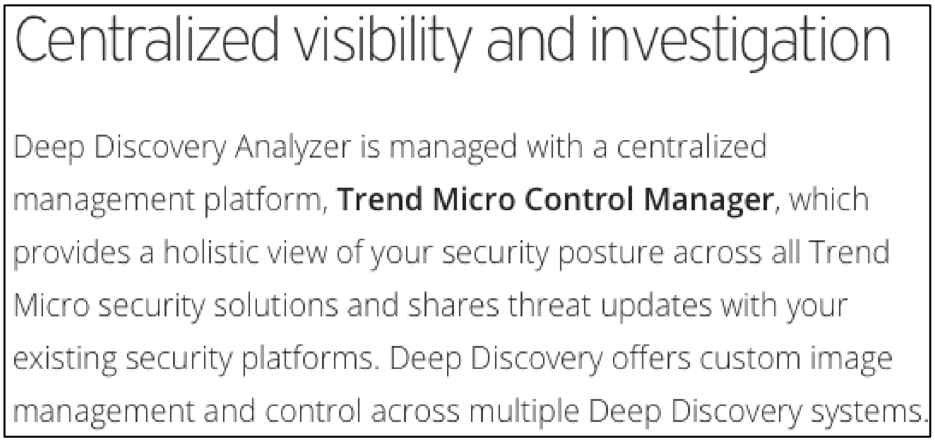
“Deep Discovery Analyzer extends the value of existing security investments from Trend Micro and third parties (through a web services API) by providing **custom sandboxing and advanced analysis.** It can also provide expanded sandboxing capabilities to other Trend Micro products. **Suspicious objects can be sent to the Analyzer sandbox for advanced analysis using multiple detection methods. If a threat is discovered, security solutions can be updated automatically.**”

Source: Deep Discovery Analyzer Dataset
https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html (emphasis added)

“Deep Discovery Analyzer is a **custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products.** Deep Discovery Analyzer supports out-of-the-box integration with Trend Micro email and web security products, and can also be used to augment or centralize the sandbox analysis of other products. **The custom sandboxing environments that can be created within Deep Discovery Analyzer precisely match target desktop software configurations — resulting in more accurate detections and fewer false positives**.

Deep Discovery Analyzer also provides a Web Services API to allow integration with any third-party product, and a manual submission feature for threat research.”

Source: https://docs.trendmicro.com/all/ent/ddan/v6.8/en-us/ddan_6.8_ag.pdf (emphasis added)



Centralized visibility and investigation

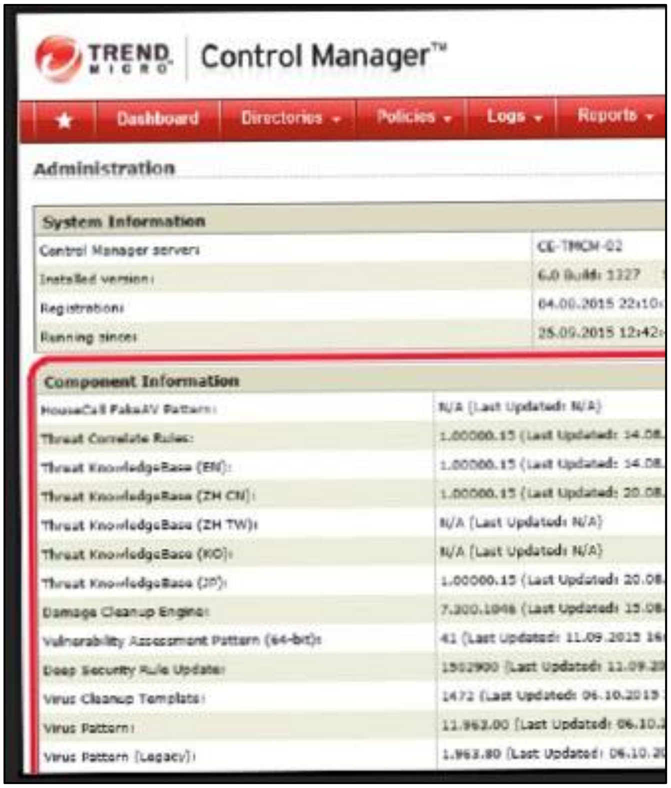
Deep Discovery Analyzer is managed with a centralized management platform, **Trend Micro Control Manager**, which provides a holistic view of your security posture across all Trend Micro security solutions and shares threat updates with your existing security platforms. Deep Discovery offers custom image management and control across multiple Deep Discovery systems.

Source: “Centralized Control” tab, https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html

U.S. Patent 7,010,698
“Systems and Methods for Creating a Code Inspection System”
Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001
Note: Statements made herein are illustrative and not exhaustive

The image below depicts an example of what Trend Micro’s Control Manager (*e.g.*, a code inspection management module) looks like.



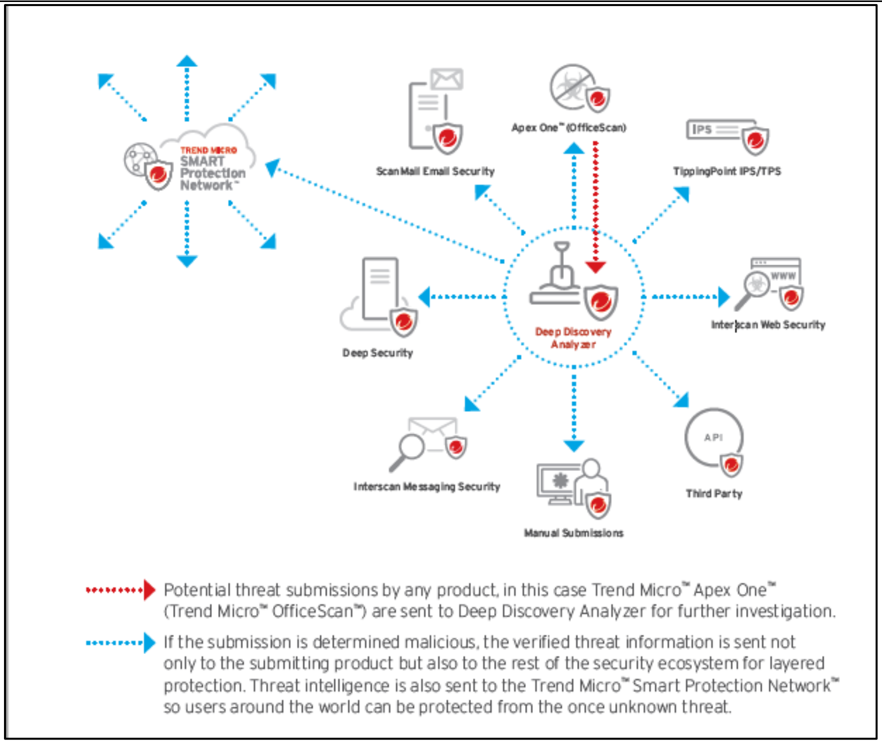
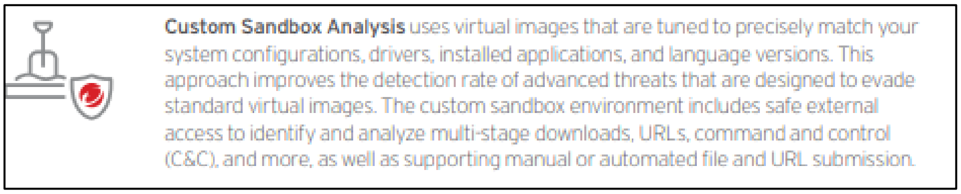
Administration

System Information	
Control Manager server:	CE-TMCM-02
Installed version:	6.0 Build: 1327
Registration:	04.00.2015 22:10
Running since:	25.09.2015 12:42

Component Information	
HouseCall FakeAV Pattern:	N/A (Last Updated: N/A)
Threat Correlate Rules:	1.00000.15 (Last Updated: 14.08.
Threat KnowledgeBase (EN):	1.00000.15 (Last Updated: 14.08.
Threat KnowledgeBase (ZH CN):	1.00000.15 (Last Updated: 20.08.
Threat KnowledgeBase (ZH TW):	N/A (Last Updated: N/A)
Threat KnowledgeBase (KO):	N/A (Last Updated: N/A)
Threat KnowledgeBase (JP):	1.00000.15 (Last Updated: 20.08.
Damage Cleanup Engine:	7.300.1046 (Last Updated: 15.08.
Vulnerability Assessment Pattern (64-bit):	41 (Last Updated: 11.09.2015 16
Deep Security Rule Update:	1502900 (Last Updated: 11.09.20
Virus Cleanup Template:	1472 (Last Updated: 06.10.2015
Virus Pattern:	11.963.00 (Last Updated: 06.10.2
Virus Pattern (Legacy):	1.963.80 (Last Updated: 06.10.20

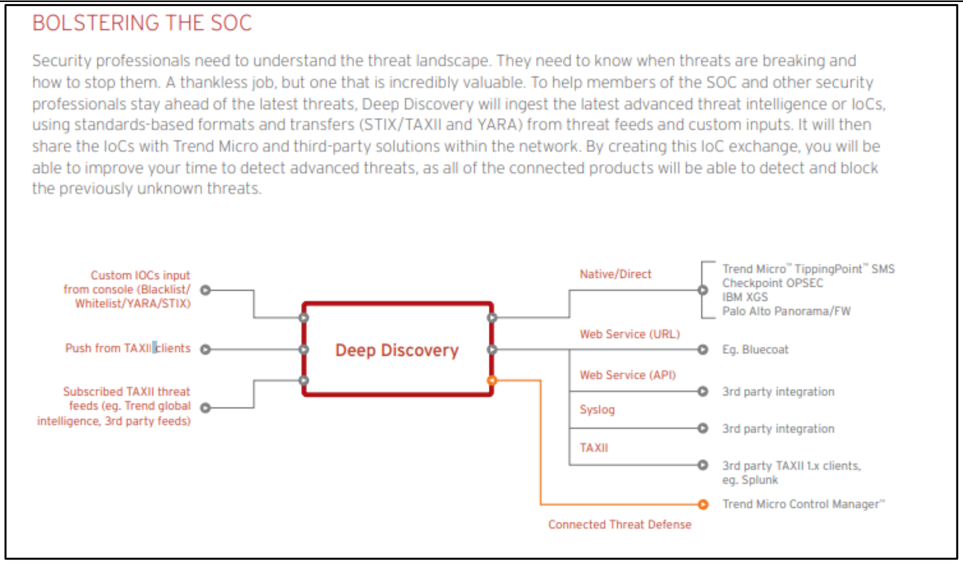
Source: “Centralized Control” tab, https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html

As shown in the diagram below, “potential threat submissions” are sent to the Deep Discovery Analyzer. If such a submission is determined to be malicious, the entire Trend Micro Security Ecosystem and Smart Protection Network is updated for all users.

	 TREND MICRO SMART Protection Network™ ScanMail Email Security Apex One™ (OfficeScan) IPS TippingPoint IPS/TPS Deep Security Deep Discovery Analyzer WWW InterScan Web Security Interscan Messaging Security Manual Submissions API Third Party Potential threat submissions by any product, in this case Trend Micro™ Apex One™ (Trend Micro™ OfficeScan™) are sent to Deep Discovery Analyzer for further investigation. If the submission is determined malicious, the verified threat information is sent not only to the submitting product but also to the rest of the security ecosystem for layered protection. Threat intelligence is also sent to the Trend Micro™ Smart Protection Network™ so users around the world can be protected from the once unknown threat. Source: “Layered Security for Detection and Response” brief, www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3b-prd-img-solution-brief-1d3c9f  **Custom Sandbox Analysis** uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more, as well as supporting manual or automated file and URL submission. Source: “Deep Discovery Analyzer,” https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html.

U.S. Patent 7,010,698
"Systems and Methods for Creating a Code Inspection System"
Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001
Note: Statements made herein are illustrative and not exhaustive



BOLSTERING THE SOC

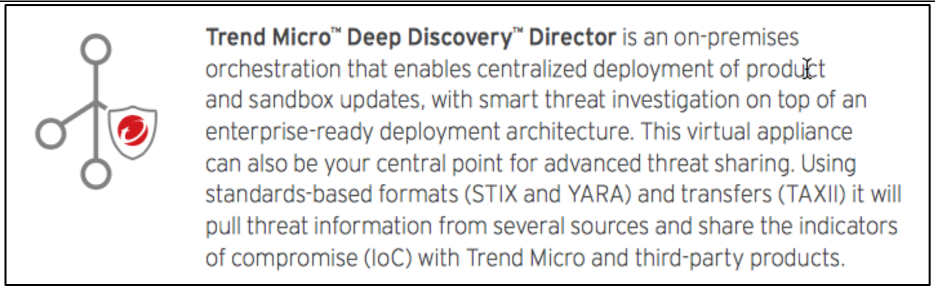
Security professionals need to understand the threat landscape. They need to know when threats are breaking and how to stop them. A thankless job, but one that is incredibly valuable. To help members of the SOC and other security professionals stay ahead of the latest threats, Deep Discovery will ingest the latest advanced threat intelligence or IoCs, using standards-based formats and transfers (STIX/TAXII and YARA) from threat feeds and custom inputs. It will then share the IoCs with Trend Micro and third-party solutions within the network. By creating this IoC exchange, you will be able to improve your time to detect advanced threats, as all of the connected products will be able to detect and block the previously unknown threats.

Custom IOCs input from console (Blacklist/ Whitelist/YARA/STIX)
Push from TAXII clients
Subscribed TAXII threat feeds (eg. Trend global intelligence, 3rd party feeds)
Deep Discovery
Native/Direct
Trend Micro™ TippingPoint™ SMS
Checkpoint OPSEC
IBM XGS
Palo Alto Panorama/FW
Web Service (URL)
Eg. Bluecoat
Web Service (API)
3rd party integration
Syslog
3rd party integration
TAXII
3rd party TAXII 1.x clients, eg. Splunk
Trend Micro Control Manager™
Connected Threat Defense

Source: "Solution Brief: Deep Discovery Family," https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/deep-discovery-threat-intelligence-network-analytics.html

For another example in the Deep Discovery Platform of products, Trend Micro offer its Deep Discovery Director (*e.g.*, code inspection management module). The Deep Discovery Director is "an **on-premises management solution** that enables centralized deployment of product updates, product upgrades, and Virtual Analyzer images to Deep Discovery products, as well as configuration replication of Deep Discovery products." Source: https://docs.trendmicro.com/en-us/enterprise/deep-discovery-director-11-online-help/introduction/about-official_produ.aspx (emphasis added).

Trend Micro describes the Virtual Analyzer as: "Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration." Source: https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf (Chapter 4).



Trend Micro™ Deep Discovery™ Director is an on-premises orchestration that enables centralized deployment of product and sandbox updates, with smart threat investigation on top of an enterprise-ready deployment architecture. This virtual appliance can also be your central point for advanced threat sharing. Using standards-based formats (STIX and YARA) and transfers (TAXII) it will pull threat information from several sources and share the indicators of compromise (IoC) with Trend Micro and third-party products.

Source: "Solution Brief: Deep Discovery Family," https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/deep-discovery-threat-intelligence-network-analytics.html

Trend Micro's Deep Discovery Director includes, *inter alia*, the following features/benefits:

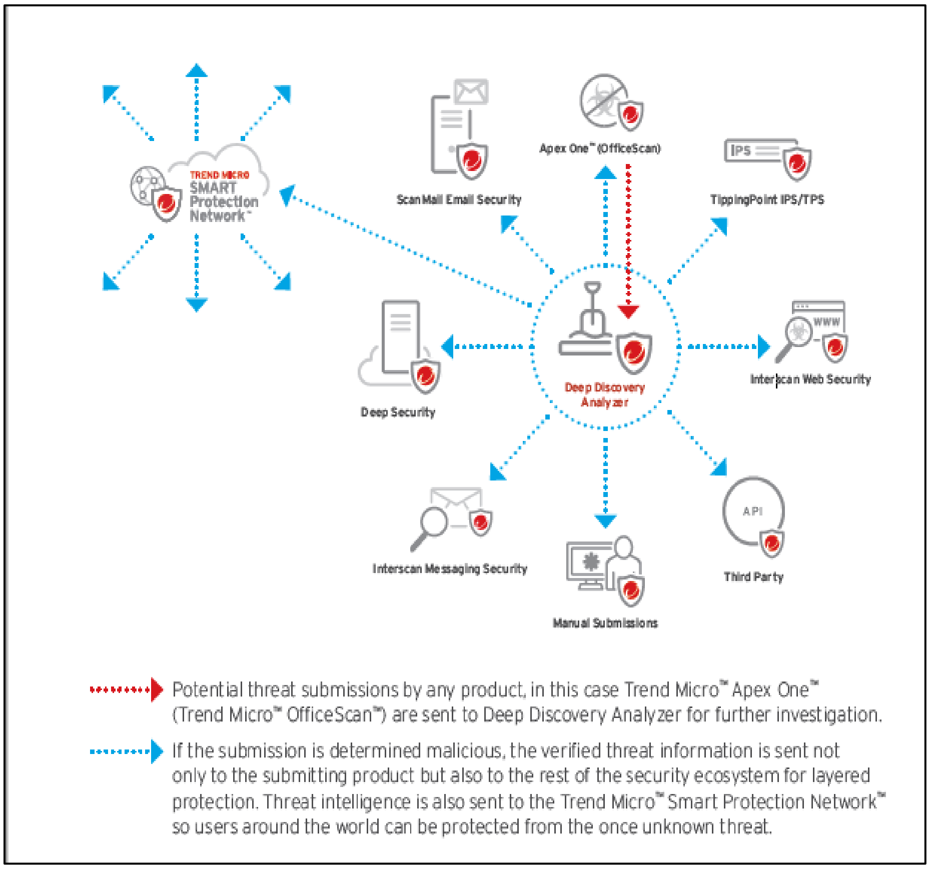
- Directory → "[D]isplays information about Deep Discovery appliances and repository servers that are registered to Deep Discovery Director."
- Plans → "[D]efine the scope and schedule of deployments to target appliances."
- Repository → "[D]isplays all update, upgrade, and Virtual Analyzer image files hosted by the server. Upload and delete files from here."
- Updates → [E]nables you to install hotfixes, patches, and firmware upgrades to Deep Discovery Director. After an official product release, Trend Micro releases updates to address issues, enhance product performance, or add new features."
- Microsoft Active Directory Integration → "Deep Discovery Director allows Active Directory accounts to access the management console."
- System Logs → "Deep Discovery Director maintains system logs that provide summaries about user access, setting changes, and other configuration modifications that occurred using the management console."

Source: https://docs.trendmicro.com/en-us/enterprise/deep-discovery-director-11-online-help/introduction/features-and-benefit.aspx

New feature updates to Deep Discovery Director include, *inter alia*:

- Virtual Analyzer Image Deployment → "Deep Discovery Director now enables the centralized deployment of Virtual Analyzer images to Deep Discovery products. To facilitate this, the Directory, Plans, and Repository screens now display additional Virtual Analyzer images related information."

	• Configuration Replication → "Deep Discovery Director now enables the centralized replication of configuration settings of Deep Discovery products. To facilitate this, the Directory, Plans, and Repository screens now display additional configuration replication related information." • Enhanced file upload options → "To facilitate the uploading of large Virtual Analyzer image files, Deep Discovery Director now enables up to three Virtual Analyzer image files to be uploaded via SFTP or network share folder at the same time." • Enhanced system logs → "The System Logs screen now enables logs to be directly readable, searchable, and filterable on the management console." • System alerts → "Deep Discovery Director monitors a variety of events and can be configured to generate alerts to inform users of those events. Alerts can be configured to be sent through email." • Firmware upgrades → "In addition to hotfixes and patches, the new Firmware screen now enables Deep Discovery Director to install firmware upgrades." Source: https://docs.trendmicro.com/en-us/enterprise/deep-discovery-director-11-online-help/introduction/whats-new.aspx
a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;	Trend Micro's accused systems embody a dynamic decoy system that, in cooperation with the code inspection module, is updated to substantially parallel relevant portions of the protected system. For example, Trend Micro's Deep Discovery Analyzer gathers potential threats from multiple sources in order to determine malicious content. If the potential threat is considered dangerous it updates the system and sends the threat information to the entire security ecosystem. The custom sandbox (*e.g.*, dynamic decoy system) matches the specific system specification (*e.g.*, protected system) in order to detect the threats.

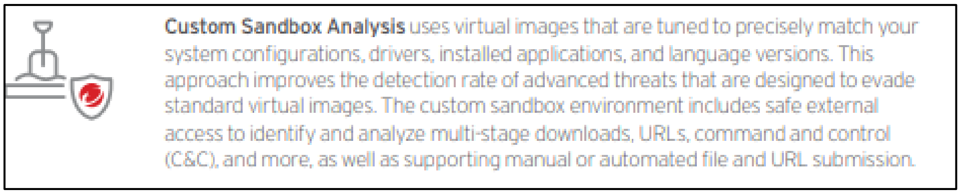


Potential threat submissions by any product, in this case Trend Micro™ Apex One™ (Trend Micro™ OfficeScan™) are sent to Deep Discovery Analyzer for further investigation.

If the submission is determined malicious, the verified threat information is sent not only to the submitting product but also to the rest of the security ecosystem for layered protection. Threat intelligence is also sent to the Trend Micro™ Smart Protection Network™ so users around the world can be protected from the once unknown threat.

Source: "Layered Security for Detection and Response" brief, www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3b-prd-img-solution-brief-1d3c9f

Trend Micro's Custom Sandbox Analysis (*e.g.*, dynamic decoy machine) uses "virtual images" that "precisely match [a user's] system configurations, drivers, installed applications, and language versions" (*e.g.*, relevant portions of the protected system).

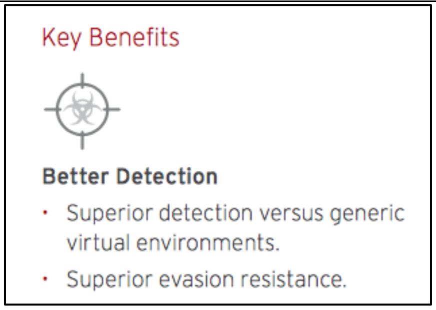
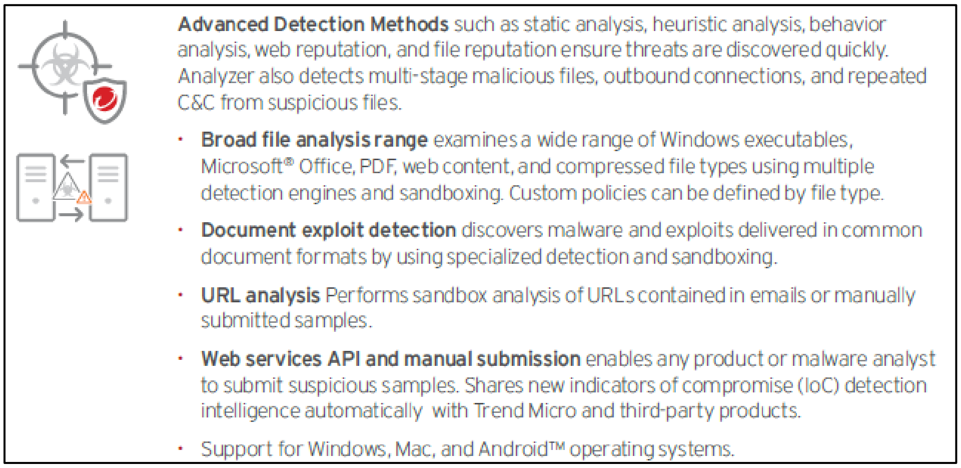


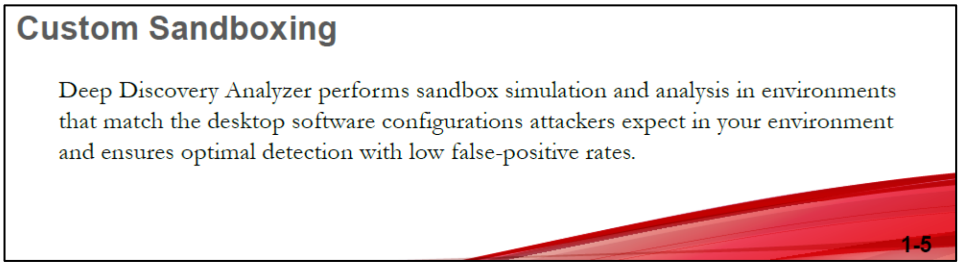
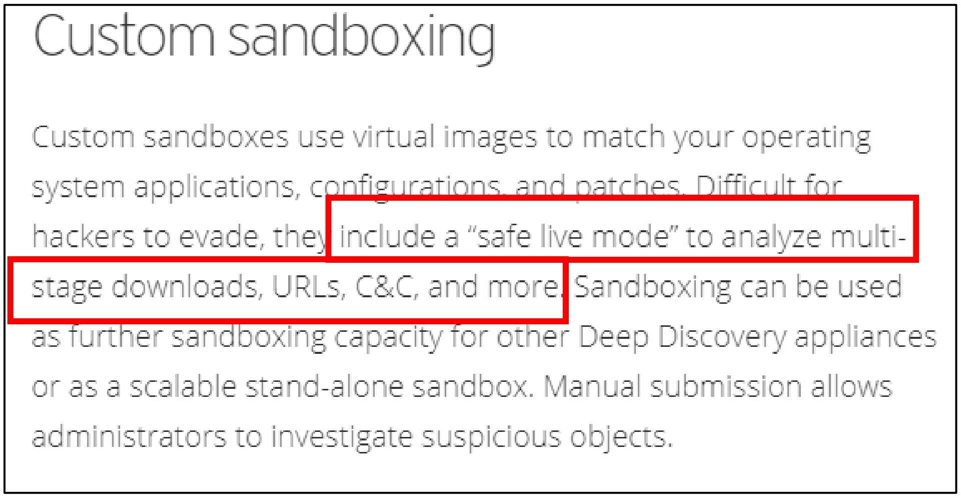
Custom Sandbox Analysis uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more, as well as supporting manual or automated file and URL submission.

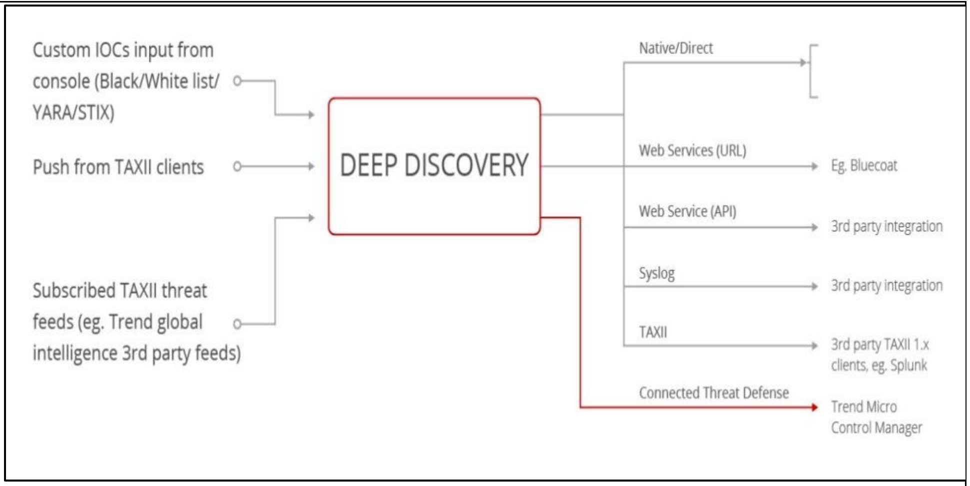
Source: "Deep Discovery Analyzer," https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html.

U.S. Patent 7,010,698
“Systems and Methods for Creating a Code Inspection System”
Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001
Note: Statements made herein are illustrative and not exhaustive

	 Key Benefits **Better Detection** · Superior detection versus generic virtual environments. · Superior evasion resistance. Source: “Deep Discovery Analyzer,” https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html.
an actuator module; and	On information and belief, Trend Micro’s accused systems embody an actuator module as claimed and as defined by the patent specification, *e.g.*, a module that “emulate[s] the normal or typical use of the protected machine, i.e., opening and closing of applications, accessing of files, or the like.” Col. 3, Lines 1-3. For example, Trend Micro’s Deep Discovery Analyzer customizable sandbox allows a wide range of executable emulation of the actual protected system, thereby requiring an actuator module. Reasonable discovery will confirm this interpretation.  **Advanced Detection Methods** such as static analysis, heuristic analysis, behavior analysis, web reputation, and file reputation ensure threats are discovered quickly. Analyzer also detects multi-stage malicious files, outbound connections, and repeated C&C from suspicious files. · **Broad file analysis range** examines a wide range of Windows executables, Microsoft® Office, PDF, web content, and compressed file types using multiple detection engines and sandboxing. Custom policies can be defined by file type. · **Document exploit detection** discovers malware and exploits delivered in common document formats by using specialized detection and sandboxing. · **URL analysis** Performs sandbox analysis of URLs contained in emails or manually submitted samples. · **Web services API and manual submission** enables any product or malware analyst to submit suspicious samples. Shares new indicators of compromise (IoC) detection intelligence automatically with Trend Micro and third-party products. · Support for Windows, Mac, and Android™ operating systems. Source: “Deep Discovery Analyzer” Datasheet, www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3a-prd-img-datasheet-679bab

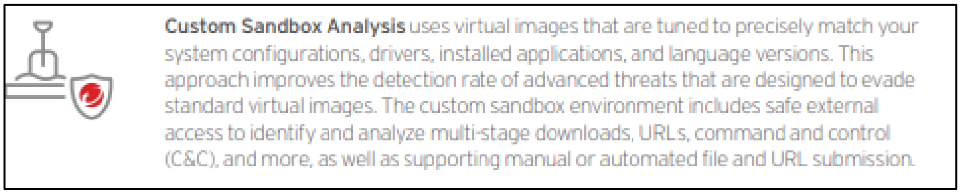
	 **Custom Sandboxing** Deep Discovery Analyzer performs sandbox simulation and analysis in environments that match the desktop software configurations attackers expect in your environment and ensures optimal detection with low false-positive rates. 1-5 Source: https://docs.trendmicro.com/all/ent/ddan/v6.8/en-us/ddan_6.8_ag.pdf  Custom sandboxing Custom sandboxes use virtual images to match your operating system applications, configurations, and patches. Difficult for hackers to evade, they include a “safe live mode” to analyze multi-stage downloads, URLs, C&C, and more. Sandboxing can be used as further sandboxing capacity for other Deep Discovery appliances or as a scalable stand-alone sandbox. Manual submission allows administrators to investigate suspicious objects. Source: “Custom Sandboxing” Tab, https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html (emphasis added)
one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of the actions and results of one or more portions of code in response to stimuli from the actuator module.	Trend Micro’s accused systems embody one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of the actions and results of one or more portions of code in response to stimuli from the actuator module. On information and belief, and for example, Trend Micro’s Deep Discovery Analyzer contains at least one or more sensor modules that is capable of analyzing the potential threats to the system. Trend Micro’s Deep Discovery system analyzes relevant, potentially malicious data, and sends relevant analyses and reports to relevant systems and users. Detection of potentially malicious data requires “one or more sensor modules.” Reasonable discovery will confirm this interpretation.


Custom IOCs input from console (Black/White list/ YARA/STIX)
Push from TAXII clients
Subscribed TAXII threat feeds (eg. Trend global intelligence 3rd party feeds)
DEEP DISCOVERY
Native/Direct
Web Services (URL)
Eg. Bluecoat
Web Service (API)
3rd party integration
Syslog
3rd party integration
TAXII
3rd party TAXII 1.x clients, eg. Splunk
Connected Threat Defense
Trend Micro Control Manager

Source: “Detect threats faster with advanced sharing,” www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/deep-discovery-threat-intelligence-network-analytics.html?modal=s5a-prd-img-deep-discovery-445d38

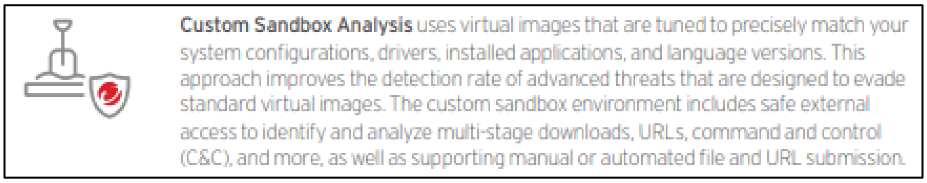
> “Organizations are increasingly becoming victims of targeted ransomware when advanced malware gets around traditional security, encrypts data, and demands payment to release the data. Deep Discovery Analyzer uses known and unknown patterns and reputation analysis to **detect** the latest ransomware attacks, including WannaCry. The customized sandbox **detects** mass file modifications, encryption behavior, and modifications to backup and restore processes.”
>
> Source: https://www.trendmicro.com/en_th/business/products/network/advanced-threat-protection/analyzer.html

Trend Micro’s Custom Sandbox Analysis (*e.g.*, dynamic decoy machine) includes “safe external access to **identify** and **analyze** . . .”



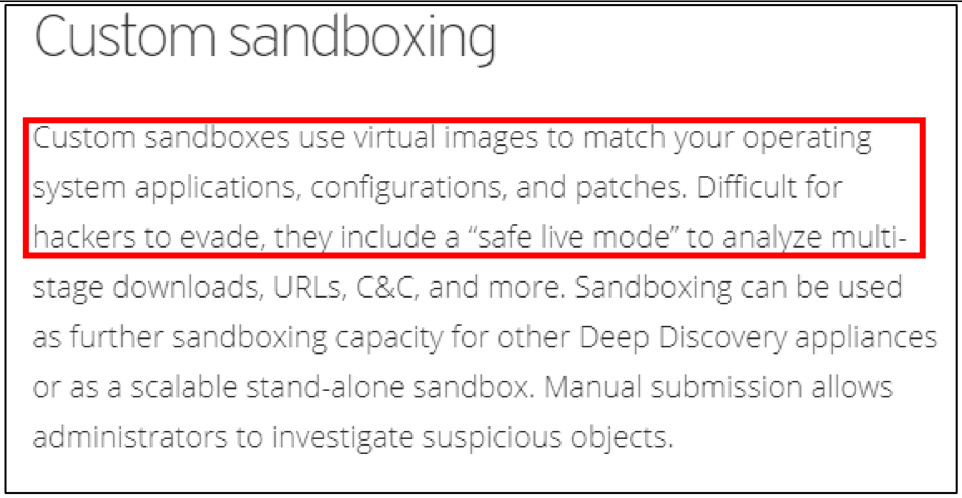
Custom Sandbox Analysis uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more, as well as supporting manual or automated file and URL submission.

Source: “Deep Discovery Analyzer,” https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html.

wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system.	Trend Micro's accused systems embody code inspection wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system. For example, Trend Micro's accused system include custom sandboxes (*e.g.*, dynamic decoy system) that use virtual images to "precisely match [a user's] system configurations, drivers, installed applications, and language versions" (*e.g.*, protected system).  **Custom Sandbox Analysis** uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more, as well as supporting manual or automated file and URL submission. Source: "Deep Discovery Analyzer," https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html. For example, in a video titled "Suspicious Objects," Trend Micro states: "analyzed in a secure custom sandbox to see what the object would do in your environment" 1:01-1:05. https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection.html For example, in a video titled "Detect lateral movement of known, unknown, and undisclosed threats," Trend Micro states: "secure custom sandbox that mimics your own corporate image down to the OS, application, version, and patches" 1:12-1:20. https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection.html

U.S. Patent 7,010,698
“Systems and Methods for Creating a Code Inspection System”
Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001
Note: Statements made herein are illustrative and not exhaustive

	 Custom sandboxing Custom sandboxes use virtual images to match your operating system applications, configurations, and patches. Difficult for hackers to evade, they include a “safe live mode” to analyze multi-stage downloads, URLs, C&C, and more. Sandboxing can be used as further sandboxing capacity for other Deep Discovery appliances or as a scalable stand-alone sandbox. Manual submission allows administrators to investigate suspicious objects. Source: “Custom Sandboxing” Tab, https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html (emphasis added)